



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Michele Veltri
Office: (267) 930-2297
Fax: (267) 930-4771
Email: mveltri@mullen.law

411 Theodore Fremd, Suite 206S
Rye, NY 10580

January 3, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Moore Holding Company (“Moore”) located at 444 Sheyenne Street, Suite 301, West Fargo, North Dakota 58078 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Moore does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 21, 2023, Moore detected suspicious activity related to certain systems within its environment. Moore took steps to secure its environment and launched an investigation to determine the nature and scope of the incident. The investigation determined that certain computer systems were subject to unauthorized access between March 20, 2023, and March 21, 2023, and that certain files stored on accessed computer systems were acquired by an unknown third party without authorization. Moore began a diligent and comprehensive review of relevant systems to determine the information that may have been impacted and to whom it related. That process completed on November 11, 2023.

The information that could have been subject to unauthorized access or acquisition includes name and Social Security number.

Notice to Maryland Resident

On or about January 3, 2024, Moore provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Moore moved quickly to investigate and respond to the incident, assess the security of Moore systems, and identify potentially affected individuals. Further, Moore notified federal law enforcement regarding the event. Moore is also working to implement additional safeguards and training to its employees. Moore is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Moore is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Moore is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Moore is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2297.

Very truly yours,



Michele Veltri of
MULLEN COUGHLIN LLC

MTV:ncl
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 3, 2024

K5854-L04-0000004 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L04 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF [Extra1]

Dear Sample A. Sample:

Moore Holding Company and Moore Engineering, Inc. (collectively, “Moore”) experienced a cyber incident that may affect the security of some of your information. This notice provides you with information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you determine it is appropriate to do so.

What Happened? On March 21, 2023, Moore detected suspicious activity related to certain systems within its environment. We took steps to secure the environment and launched an investigation to determine the nature and scope of the incident. On April 4, 2023, the investigation determined that certain computer systems were subject to unauthorized access between March 20, 2023, and March 21, 2023, and that certain files stored on accessed computer systems were acquired by an unknown third party without authorization.

What Information Was Involved? Moore began a diligent and comprehensive review of relevant systems to determine the information that may have been impacted. On November 11, 2023, we determined that certain information related to you was stored on the impacted systems. The information that may have been impacted by this incident includes your name in combination with [Extra2]. At this time, we have no indication that your information was subject to actual or attempted misuse in connection with this incident.

What We Are Doing. Moore takes this incident and the security of information within our care very seriously. Upon discovery of this incident, we immediately launched an in-depth investigation to determine the full nature and scope of this incident. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our existing security policies and procedures, and we are working to implement additional security measures to further protect against similar incidents in the future. We are also notifying state regulators, as required.

Although we are not aware of any actual or attempted misuse of your information, as an added precaution, we would like to offer you 12 months of complimentary access to credit monitoring services through Experian. If you wish to receive these services, you must enroll by following the enrollment instructions below, as we are not allowed to activate these services on your behalf.



What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports to detect errors or suspicious activity over the next twelve (12) to twenty-four (24) months. You can find more information about how to get a free copy of your credit report, as well as additional resources available to you to help protect your information from possible misuse in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find information on how to enroll in the complimentary credit monitoring services we are offering you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please contact us at 833-420-2884, toll-free Monday through Friday from 8 am – 8 pm CST (excluding major U.S. holidays). Please be prepared to provide your engagement number B112219.

Sincerely,

Shane Waslaski
CEO
Moore Holding Company

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by March 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-420-2884 by March 31, 2024. Be prepared to provide engagement number B112219 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.



Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.